The Claims

1. (Currently amended) A registration authority comprising:

a protocol converter coupled to receive messages from a router targeting a certificate authority, and to receive messages from the certificate authority targeting the router;

a request hash table configured to maintain a mapping of certificate authority request IDs to hash values of the router requests;

wherein the protocol converter is configured to convert the messages received from the router in accordance with a first protocol and convert the messages received from the router to a second protocol and subsequently communicate the converted messages to the certificate authority; and

wherein the protocol converter is further configured to convert the messages received from the certificate authority in accordance with the second protocol and convert the messages received from the certificate authority to the first protocol and subsequently communicate the converted messages to the router.

2. (Original) A registration authority as recited in claim 1, wherein the registration authority is independent of the certificate authority.

3. (Original) A registration authority as recited in claim 1, wherein the first protocol is a Simple Certificate Enrollment Protocol (SCEP) enrollment protocol.

4. (Original) A registration authority as recited in claim 1, wherein the second protocol is a Public-Key Cryptography Standards (PKCS) enrollment protocol.

5. (Original) A registration authority as recited in claim 1, wherein the registration authority conforms to the network Working Group Request for Comments 2459 standard.

6. (Original) A registration authority as recited in claim 1, wherein the messages received from the router comprise one or more of: a router enrollment message, a get certificate revocation list (CRL) message, a get certificate message, and a get certificate authority (CA) certificate message.

7. (Original) A registration authority as recited in claim 1, wherein each message received from the certificate authority comprises a response to a message received by the registration authority from the router.

8. (Original) A registration authority as recited in claim 1, wherein the router is unaware that it is communicating with a registration authority rather than directly with the certificate authority.

9. (Original) A registration authority as recited in claim 1, further comprising a transaction ID table configured to maintain a mapping of router transaction IDs received from the router to certificate authority request IDs received from the certificate authority.

10. (Canceled).

11. (Original) A registration authority as recited in claim 1, further comprising a password table configured to maintain a valid password issued to the router.

12. (Original) A registration authority as recited in claim 1, further comprising a module configured to receive a request for a certificate of the certificate authority and, in response to the request, return a certificate of the registration authority.

13. (Original) A registration authority as recited in claim 12, wherein the registration authority is a dynamically linked library.

Claims 14-16. (Canceled).

17. (Currently amended) One or more computer-readable media having stored thereon a computer program that, when executed by one or more processors of a registration authority, causes the one or more processors to perform acts including:

receiving, from a device, a first message in accordance with a first protocol, wherein the first message comprises an enrollment message;

generating, based on the first message, a second message in accordance with a second protocol;

sending the second message to a certificate authority;

receiving, from the certificate authority, a third message in response to the second message and in accordance with the second protocol, wherein the third message comprises a certificate authority pending response;

generating, based on the third message, a fourth message in accordance with the first protocol; ~~and~~

sending the fourth message to the device as a response to the first message; and

wherein the computer program further causes the one or more processors to perform acts, in response to the certificate authority pending response, generating:

a hash value based on the enrollment message;

a hash table entry mapping a pending response ID, corresponding to the certificate authority pending response, to the hash value; and

a transaction ID table entry mapping the transaction ID, corresponding to the enrollment message, to a pending response ID corresponding to the certificate authority pending response.

18. (Original) One or more computer readable media as recited in claim 17, wherein the device comprises a router.

19. (Canceled).

20. (Currently amended) One or more computer-readable media as recited in claim [[19]]17, wherein generating the second message comprises:

verifying that the first message has been digitally signed by the device;

decrypting the first message;

extracting a certificate enrollment request from the first message;

generating a certificate authority request including the certificate enrollment request and a subject alternative names extension; and

creating the second message by digitally signing the certificate authority request.

Claims 21-24. (Canceled).

25. (Currently amended) One or more computer-readable media as recited in claim [[24]]17, wherein generating the fourth message comprises:

generating a pending response;

encrypting the pending response; and

creating the fourth message by digitally signing the encrypted pending response.

26. (Canceled).

27. (Currently amended) One or more computer-readable media as recited in claim [[26]]17, wherein the computer program further causes the one or more processors to perform acts including:

receiving an additional enrollment message from the device;

accessing the transaction ID table to obtain the pending response ID corresponding to the additional enrollment message; and

transmitting, to the certificate authority, a certificate request including the pending response ID.

28. (Currently amended) One or more computer-readable media as recited in claim [[26]]17, wherein the computer program further causes the one or more processors to perform acts including:

receiving an additional enrollment message from the device;

generating a new hash value based on the additional enrollment message;

checking whether an entry in the hash table matches the new hash value; and

if an entry in the hash table matches the new hash value, then,

obtaining a pending response ID, from the hash table, corresponding to the new hash value, and

transmitting, to the certificate authority, a certificate request including the pending response ID.

29. (Currently amended) One or more computer-readable media as recited in claim [[26]]17, wherein the computer program further causes the one or more processors to perform acts including:

maintaining the hash table entry in the hash table for a selected amount of time.

30. (Currently amended) One or more computer-readable media as recited in claim [[26]]17, wherein the computer program further causes the one or more processors to perform acts including:

maintaining the transaction ID table entry in the transaction ID table for a selected amount of time.

Claims 31-56. (Canceled).